NAVAL SEA SYSTEMS COMMAND

SHADOW

SECONDARY HEURISTIC ANALYSIS FOR DEFENSIVE ONLINE WARFARE

NAVSEA
DAHLGREN
Surface Warfare Center Division

NAVAL SURFACE WARFARE CENTER, DAHLGREN DIVISION

DAHLGREN PANAMA CITY DAM NECK

Overview

Twenty-first century warfare will be fought not only on the battlefields, but in the information arena. Already, individuals and organizations are conducting offensive information operations against network systems used by the Department of Defense (DOD), other Government agencies, corporations, and other institutions. Providing protection from intrusion by hackers, both the casual and professional, is critical to the security of all organizations. Currently, attacks on information systems happen because intruders take advantage of the vulnerabilities existing in the current network service systems.

To combat this threat, the Navy, with funding from several sources, including Ballistic Missile Defense Organization, Office of Naval Research (ONR), and security at Naval Surface Warfare Center, Dahlgren Division (NSWCDD), has tasked engineers at NSWCDD to develop a multi-site network based intrusion detection system (IDS). In response, the team developed the ***S****econdary* ***H****euristic* ***A****nalysis for* ***D****efensive* ***O****nline* ***W****arfare (SHADOW) system designed to detect computer network attacks efficiently, report any possible attacks quickly, and provide analytic capabilities to help prevent future intrusions.*

Currently, the basic SHADOW system is available at no cost via the internet. Custom enhancements for other Federal Agencies or corporations are available on a cost reimbursement basis.

How SHADOW Works

Unlike most commercial security systems available on the market, *SHADOW* does not open the contents of network communications packets to check for key words which may indicate a security problem is developing. Rather, *SHADOW* tracks, filters and analyzes all network traffic by reviewing records on an hourly basis and providing the analyst with a summary report. An inappropriate destination address, strange routing, or an overabundance of traffic from a single source will cause that activity to be noted in the hourly SHADOW report.

SHADOW serves as a baseline intrusion detection and network security tool for many DoD and other Federal agencies. It is also used by private sector organizations internationally.

Using only two personal computers, one on each side of the network firewall, *SHADOW* senses, monitors, and analyzes all incoming network traffic. Outside the firewall, *SHADOW* records all network traffic, forwarding it to the inside analysis station and then displaying those which are questionable. Inside the firewall, *SHADOW* analyzes the information and alerts the local security analyst that a problem may exist. It tracks and prints out on a regular basis network traffic records which indicate malicious activity.

SHADOW is very cost effective to use. All software on both the sensor computer outside the firewall and the analysis station inside the firewall is freeware or government written. The *SHADOW* system is freely available over the internet. Training is available through the System Administration and Network Security (SANS) Institute.

Future Developments

The NSWC *SHADOW* team are working to improve the effectiveness and ease of use of *SHADOW*. Some of the areas of upcoming improvement are:

- Incorporation of statistical anomaly detection
- Incorporation of basic visualization techniques
- Re-engineering *SHADOW* to:
  - Develop a tcp state machine
  - Process information in real-time
  - Develop database analysis
- Protecting against insider threat
- Develop *Dark* **SHADOW**, a software system to correlate multi-site databases to discover/detect attacks whose signatures are so small at any one location, they can not now be detected.

> *It's NOT a matter of whether America*
> *will have an electronic Pearl Harbor . . .*
> ***it's a matter of when.***
>
> *Congressman Curt Weldon, Republican, Pennsylvania*

What SHADOW Detects

SHADOW is designed to detect, before it becomes a problem, the following types of potential intrusions:

- Denial of service attacks
- Network mapping
- Unauthorized use
- Common exploits
- Abnormal activity

Awards/Recognition

Recognized and respected as a leader in intrusion detection and network traffic analysis, the *SHADOW* team received the Government Technology Award in 1998. The team's innovations have been covered by magazines such as *Information Week, PC Week, Sci-Tech News, SunWorld, Government Computer News* as well as CNN Online, ABC Online, Wired and Live Webcasts.

Thousands of internet sites already are using *SHADOW*. Federal recognition from the Defense Advanced Research Projects Agency (DARPA), DoD, and FED-CIRC indicate how important *SHADOW* has become to the security of DoD and the nation's networking systems.

NAVSEA
DAHLGREN
Surface Warfare Center Division

NSWCDD/MP-99/120: 2/00
Approved for public release; distribution is unlimited.

For additional information, please contact:

NSWCDD Public Affairs
Telephone: (540) 653-8153
Internet: www.nswc.navy.mil

We are looking for scientists and engineers in different fields.
For employment opportunities, please send your resume to:

NSWCDD College Recruiting Program
Human Resources Department, Code PD
17320 Dahlgren Road
Dahlgren, VA 22448-5100

Telephone: 1-800-352-7967
E-mail: recruit@nswc.navy.mil
Internet: www.nswc.navy.mil/P/RECRUIT/recruit.html